1 Problem 1

1.1 What is GDPR?

The **General Data Protection Regulation (GDPR)** is a legal regulation in EU law pertaining to the protection of data within the European Union and the European Economic Area (EEA), and the protection of this data when it is transferred out of this region. GDPR applies to any organisation that is processing the personal data of individuals who are in the EEA, regardless of the location of said organisation or the citizenship / residence status of the individuals whose data is being processed. GDPR sets out several key principles in relation to the processing of personal data:

- **Lawfulness -** You must identify a *lawful basis* under the GDPR for the processing of personal data.
- **Fairness & Transparency -** You must be open & honest with the Data Subjects about how and why their data is being processed, and you must not use this data in a way that doesn't align with these methods.
- **Purpose Limitation -** You must clearly state your purposes for processing the personal data of Data Subjects from the start, and may only use the data for different purpose if it is either compatible with your original purpose, you get *consent*, or if you have a *clear basis* in law.
- **Data Minimisation -** The personal data you process must be *adequate*, *relevant*, and *limited* only to what is necessary.
- **Accuracy -** Personal data should not be incorrect or misleading.
- **Storage Limitation -** You must not keep personal data for longer than you need it.
- **Integrity & Confidentiality -** You must take appropriate technical & organisational measures to ensure that the personal data of data subjects remains *secure*.
- **Accountability -** You must be able to demonstrate your compliance with GDPR.

All Data Processors (i.e., anyone who is responsible for the processing of personal information) are motivated to obey GDPR by threat of strict penalties. For particularly serious GDPR breaches, a Data Processor could be fined up to €20 million, or 4% of the firm's global turnover. For less serious breaches, the Data Processor can be fined up to €10 million, or 2% of the firm's global turnover.

1.2 Why was GDPR introduced? What was the motivation for this legislation?

GDPR was introduced with the aim of enhancing the rights & control of individuals over their personal data and to simplify data processing regulations with regards to international businesses.

As the processing of the personal data of individuals increases in the modern world with the advent of modern technology, it has became necessary to update the laws governing the processing of personal data to protect the interests of data subjects in an era of unprecedented data collection, surveillance, & processing. GDPR sets out clear & concise principles & rules that determine who's personal data may be processed, what information this data may consist of, when it is acceptable to process it, where this data can be processed & relocated to, why this data may or may not be processed, and how this data processing can be undertaken.

The European Parliament adopted the GDPR in April 2016 to replace the then-outdated Data Protection Directive, which was first enacted in 1995. There were 2 main issues with the Data Protection Directive that made it necessary to replace it:

1. Under EU law, a "Directive" is less strict than a "Regulation". A Directive allows the EU member states to adapt & change the law to fit the needs of their citizens, while a Regulation does not allow this. A Regulation forces the member states to adopt it, and does not allow them to adapt or change it at all.
2. The Data Protection Directive was too outdated for the modern world. It did not address how data is collected, stored, or transferred in the digital world, and thus largely failed to regulate digital data processing.

2 Problem 2

This company needs to be extremely careful with their GDPR compliance, as they are handling some extremely sensitive personal information.

With regards to the GDPR key principle of **Lawfulness**, I think that this website is in the clear. Since the users are uploading their own data of their own volition, this gives the website a clear lawful basis for data processing - they have the *consent* of the data subjects for the processing of their data.

I do, however, have some concerns about the compliance of the company with GDPR key principle **Fairness & Transparency**. The company is quite vague about how they process the personal data of the users, how the data is stored, etc. There is no mention of any kind of Data Protection Notice that informs the user of the identity & contact details of the Data Controller, the contact details of the Data Protection officer, the details of any data transfer out of of the EEA or the safeguards in place, the data retention period, or the individual's rights. The only information that the Data Subjects really have is the purpose of the processing and (at least some of) the recipients of the data. It's possible that other people are in receipt of the users' personal data as well, but there is no mention of this.

The company should be in the clear with regards to **Purpose Limitation**, assuming that they are being fully open & honest about their purposes for processing the data, and stick to these purposes, but if they are not doing this, then that is a massive issue.

The principle of **Data Minimisation** is a bit more of a grey area for this website. It's hard to say what data is and isn't adequate & relevant to the purpose of "keeping in touch". Personally, I would be of the opinion that absolutely none of the data mentioned is relevant for the purposes of "keeping in touch", but it is plausible that some people would feel otherwise. It could be problematic for the company that they allow the users to upload pretty much whatever they want, as the company may end up in possession of a lot of irrelevant data that the users uploaded. The company needs to be extremely careful with receiving data that they didn't expect to receive, which may or may not be relevant to the purposes of the company.

The principle of **Accuracy** is another potentially problematic one for this company. The company must take all reasonable steps to ensure that the personal data that they hold is not incorrect or misleading as to any matter of fact. It's not unlikely that some, if not many, of the users of the website will "exaggerate" (or just make up) positive aspects of their life after university, their salary, etc. There also doesn't seem to be any protocol to verify that the users are who they say they are, so anyone could be uploading the personal data, fictitious or otherwise, of anyone else, and this data could be viewed by anyone in the world, so long as they claimed to be an alumni of a particular course. This is a problem for the company, as they have the responsibility to ensure that the data is accurate, although this may be considered to be something that the company cannot reasonably be expected to regulate / control.

The company does not seem to comply with the principle of **Storage Limitation** at all. There is no mention of data retention period, or how the users might be able to learn their data retention periods.

Similarly, the company doesn't seem to comply with **Accountability & Governance** at all either. There is no attempt to provide an assurance of GDPR compliance, or to explain why the data is held, when it will be deleted, and who may gain access to it.

There is no mention of any attempt to comply with **Integrity & Confidentiality** either. There is no mention of any security measure such as encryption, nor do they mention any other technical measures that they might use to process the data securely.

3 References

1. Schukat, M. (2022-09-09). *CT255 Lecture Slides - GDPR.* Blackboard.
2. Wolford, B. *What is GDPR, the EU's new data protection law?* Proton. https://gdpr.eu/what-is-gdpr/
3. Sivula, A. *GDPR: What Happens If You Don't Comply*. AMD Solicitors. https://amdsolicitors.com/gdpr-what-happens-if-you-dont-comply/

4. Rossow, A. *The Birth of GDPR: What Is It And What You Need To Know*. Forbes https://www.forbes.com/sites/andrewrossow/2018/05/25/the-birth-of-gdpr-what-is-it-and-what-you-need-to-know/?sh=62b80a5a55e5